Minimization of System Resources for Cloud based Application using Web Browser Add On

Meduri Jagadeesh[#], R.K.Nadesh[*]
School of Information Technology and Engineering, VIT University
Vellore - 632014, Tamilnadu, India.
#P.G.Scholar,*Assistant Professor(Senior)
meduri.jagadeesh@msn.com, rknadesh@vit.ac.in

***Abstract*— Evolution of cloud makes users to manage the data and applications online. It is the responsibility of the cloud service providers to care of data secure in terms of transferring and efficient by providing reliable performance. There are many challenges that are faced by the service providers to achieve the trust of the user. User feels insecure while the data is send to the cloud servers, when the data is more confident and uses applications that provide security to the data (by encryption and decryption). These applications to encrypt data will consume more time and systems resources. All these applications work depending upon the operating system of the user. This proposed approach will reduce user's burden in interacting to the cloud through browsers add-on. This add-on is designed by AES encryption methodology with a SHA-2 key which is proved to be secure. The main aim of this paper is to explore various environments and design cloud based applications which are more user friendly at the same time reduce hardware cost. This design also highlights a threat to the mailing servers as they can't find the transmitting information from the user**.

Keywords- Operating System, Advanced Encryption Standard , Secure Hash Algorithm.

1. INTRODUCTION

Emerging of cloud applications minimizes the hardware cost and minimizes the server maintenance over head. All these factors may affect the security and raise vulnerabilities. Attacks may compromise security factors like confidentiality, integrity and authentication. Research scholars developed many mechanisms to achieve these security factors in dealing the data on the cloud. Author [9] explains the required security measures a cloud should posses. These models involve cryptographic techniques that provide security. The mechanism by [15] shows the user completely depend on third party broker to secure his data. The design reduces the user's burden but raises a threat from third party. There is need for a mechanism which reduces users accessing burden and also posses enhanced security. These models involve cryptographic techniques that provide security. Secret key algorithms improve performance and the hashing algorithms create fixed hash to check the integrity. Theoretical and practical collisions are proved on MD5 and SHA-1 which are proven to be unsecure and they have collisions.

Distributed systems are widely developed all over the Internet. Cloud computing grows along with distributed environment. Distributed systems made cloud to add its features to the web and make them to be used by user in different parts of the distributed environment by just having internet connection. They are able to access different cloud resources with same speed as provided by their cloud service provider. Mechanisms [5, 6] designs security mechanism to Windows, Linux and smart phone but people will use different operating system based on their usage capability. The problems like unsupported format while accessing the files may arise from a different operating system. In order to make those files support for user operating system they need to install some applications to convert a particular file.

The mail servers will read user's mail. That's why we can see the advertisements when one open the mail which relates to our action. This shows a user is not in absolutely private with his mail and dangerous activities can be monitored. In order to send some secure information in mail like Credit card details user feel unsecure. This shows necessity for unreadable format of data for sending and receiving to achieve confidentiality.

2. PROBLEM DEFINITION

Application oriented Encryption and decryption is a tidy process to achieve. Taking to the cloud environment where the data is transferred to multiple and different machines, the task become more serious in terms of performance. Thus there is a need for a mechanism which can effectively encrypt and decrypt the files in any operating system. There is no efficient mechanism that provides security in terms of confidentiality, integrity, authentication along with distributed environment support.

The problem above is now explained with the following example. A and B are two friends want to share some secret information through mail. They feel there may be tampering while sending through mail and decided to encrypt the data and before transfer. Thus A used an application called MEO (software used for encryption and decryption) on message and sends it to B. He shares the secret by making a call or sending a text message to B's mobile. Now B has to download the MEO software and decrypt the file. This Procedure is time taking and may waste system memory resources. The case will be worst in case of B is using MAC book or Linux Operating System.

3. LITERATURE SURVEY

In cloud, web browser is an important tool with its own features. Extra features needed by user can be added to the browser through a mechanism called Add-on.

Author [1] designed a model in which user can ensure his data with the cloud and misbehavior on the cloud can be detected. In this model a third party auditor is used who may compromise the security of the user.

Author [2] explains various security attacks in cloud and a security model against DOS (Denial of Service) attacks. Author provides the solutions for access control in cloud solutions, incident countermeasure and response that provides partitioning, migration, work analysis and allocation.

Author [3] surveyed proactive redundant attacks in cloud and divided security accepts as trust, risks, issues and threats and explains an application should tolerate to this aspects.

A survey by author [4] describes the various security measures used in cloud computing to ensure Cloud environment. He successfully explains cloud and users architectures and how they access each other using cryptographic techniques.

Author [5] analyzed security of cloud deploying in Windows 7 and Linux operating systems. The analysis shows that data security and privacy are the major two aspects dealing with the OS security. The paper shows the need of developing more user friendly environment to the users of particular OS in dealing with the cloud.

Author [6] designed a security solution for smart phones by a lightweight process. This model continuously updated by connecting to network so that it interacts with cloud where security module exists. The services include call monitoring, integrity checking and instruction detection with response.

Author [7] designed a tree based key management where multiple parties hold the rights. Here multiple keys are generated for multiple parties. Here user indirectly stores his data with private enterprise cloud and risks his data by providing it to the public cloud that contact the enterprise cloud.

Author [8] provides a communication protocol along with mathematical analysis which provides the confidentiality for the user. But the client has to completely relay on the Service provider.

Author [9] gives a model which manages cloud security and gave the necessity of key security mechanisms that are required for cloud computing.

Author [10] proposed a model which provides major security requirements like confidentiality, availability and integrity using a three layer security model. He simulated his results in Hadoop. But coming to implementation the job is tidy and increases the access time.

Author [11] made a survey on cryptographic techniques used in cloud computing using Pseudo random number generator and determines the most suitable technique that can be used for his scenario. The algorithms are selected based on NIST's statistical testing in cloud computing environment.

Author [12] explains attribute based encryption and proxy based re-encryption and designed a time based schemas for them and provide access rights to the Cloud service provider. The design involves tree based key generation for successive time periods.

Author [13] analyzed the vulnerabilities in applications life cycle of Amazon, Google and VMware. Author designed framework to connect cloud and developed a lifecycle that enhances the security in cloud applications.

A method of homomorphic encryption is developed by author [14] is using the method which will make service provider tough to access our data and meanwhile can perform operations on raw data without decryption.

Author [15] proposed an Integrity check on cloud for users by using a third party administrator. Third party broker will segment and decrypt the data and send to the cloud service provider. This model completely throws the burden to the broker and at the same time compromises the security of user.

Author [16] successfully announced AES algorithm which provide enhanced security of data compared to previous cryptographic algorithms. Its versions are 128/192/256 bit with rounds 10/12/14 key size. Author provides strategy to design the AES algorithm in Java Script. The papers also give brief strategy about rounds, key generation and phases of AES.

4. PROPOSED WORK

The main aim is to achieve a distributed environment that will be well suited for any operating system to avail security to archive security flaws. The algorithms used in proposed model are AES and SHA. Algorithm complexity is increased by using SHA.

The overview of the proposed system is to build an Add-On for Mozilla Firefox web browser that provides security to the data while transferring through online. This add-on is used in any operating system with Coding of the add-on done using HTML, CSS (Cascading Style Sheet), and JavaScript. The Encryption and decryption of AES is done in JavaScript. HTML used to access the content in the browser for encryption. CSS provides styles for the Add-on.

Design: It deals with the designing of the add-on for Firefox. The designing of the add-on is on open source programming. The implementation is done using JavaScript, Html and CSS. The entire encryption algorithm is implemented using Java Script. CSS will help in working with the add-on in any user friendly environment.

Structure of Add-on: The structure of the add-on will be in zip format. For Firefox it is in XPI (Extended Process Integration). This extension having a structure which will help in placing our code in an exact model as required by the format. The following figure shows the format of the XPI file.

The main contents in XPI are:

- Chrome
- Defaults
- Locale
- Skin

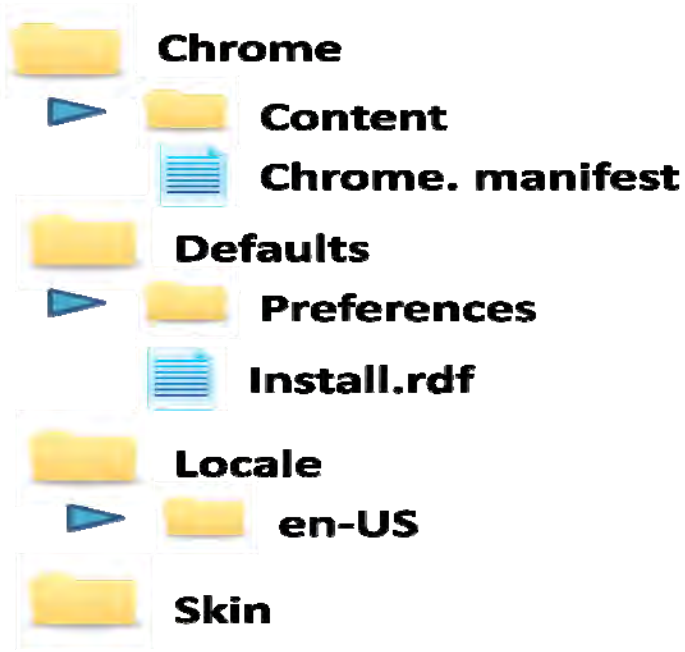

Figure 1: XPI file format

Chrome: This chrome file is the heart of the Add-on. It contains content folder and chrome. Manifest file. The content folder is the heart of the Add-on having the implementation files. Here Java Script code is used for add-on creation. Here chrome. Manifest deals with the designing of the add-on features in menu and status bar of the browser. Here we can specify the path how the next file of the Add-on will be accessed while running the Add-on.

Defaults: Here the preferences like shortcuts for the add-on operations can be set as user friendly. The install.rdf (resource description framework) file is another default file which should be filled by user. It contains the compatibility details of the Add-on. The other details like version, name, description and supporting versions for the add-on are given here.

Locale: This file is having the language specification of the add-on. Here additional languages can be added for user friendly environment by translation.

Skin: The skin folder consists of the images used in the Add-on for gentle display. They will be added in to the add-on by specifying the path in the chrome main content folders main file. The images must be registered in chrome .manifest file.

Algorithm used:

AES:

Of all the encryption schemas AES provides more secure and its versions are still stronger. It treats data in 4 groups of 4 bytes. It is almost resistant against all known attacks. It is a secret key algorithm which makes it faster than public key algorithms. In order to increase the key complexity, the hash of the secret key is used by AES in this add-on. This will increase the confidentiality of the message. In order to maximize the performance AES is designed in counter mode which will decrease the padding burden by adding the counter.

SHA:

Of all the one way hash algorithms SHA-256 is still now secure and no practical collisions are found. In this add-on SHA-256 hash is generated for the secret key and the hash is used as a key to AES input. This makes attacker, though he find secret key and not able to decrypt it, as hash is used as key for decryption.

Complexity:

Here the complexity is, we can use any of the encryption algorithms according to user choice. Hash is used further for making the environment more complex. Using, this type of add-on in mailing make the Service provider unable to the message of the user. The following cases explains, this approach acts secure

Case (1): When the message is tampered: They can't understand as it is encrypted. Though intruder has some decryption mechanisms he can't find which algorithm the sender is using.

Case (2): When the attacker has the secret key and decryption mechanism: He can't decrypt as we are using hash as key instead of original key for encryption.

Encryption: The following figure shows the decryption procedure where the encrypted message from cloud server is decrypted by secret key's hash. Counter mode of operation increases the performance.

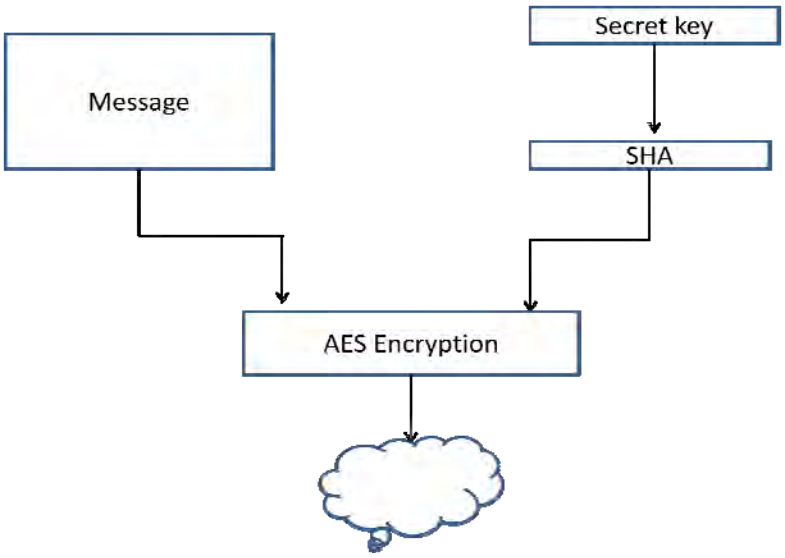

Fig. 2. Encryption Methodology

Decryption:

The decryption process will be in counter mode and as reverse of encryption by using secret keys hash.

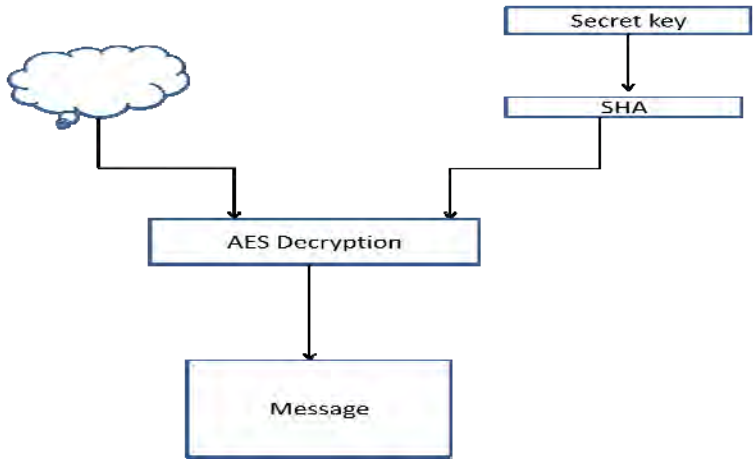

Fig.3 Decryption Methodology

5. IMPLEMENTATION

The Add-on (.xpi) is as per the model designed above and is dragged on to the browser where the browser automatically restarts. The add-on is designed in such a way that it can access the text area of the html document. Figure 4 shows the encryption mechanism where password is given for encryption

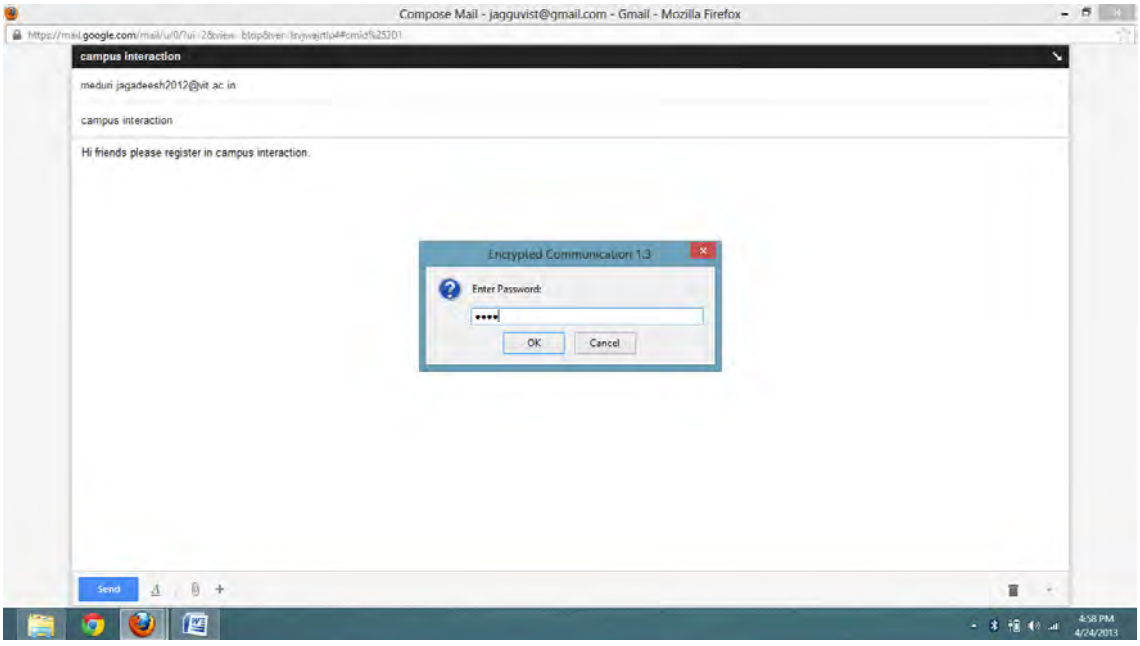

Fig 4 Encryption by password

The receiver on his mail opens the and selects the data with the decrypt option by entering the password, the data will be decrypted as shown in fig 5 and fig 6.

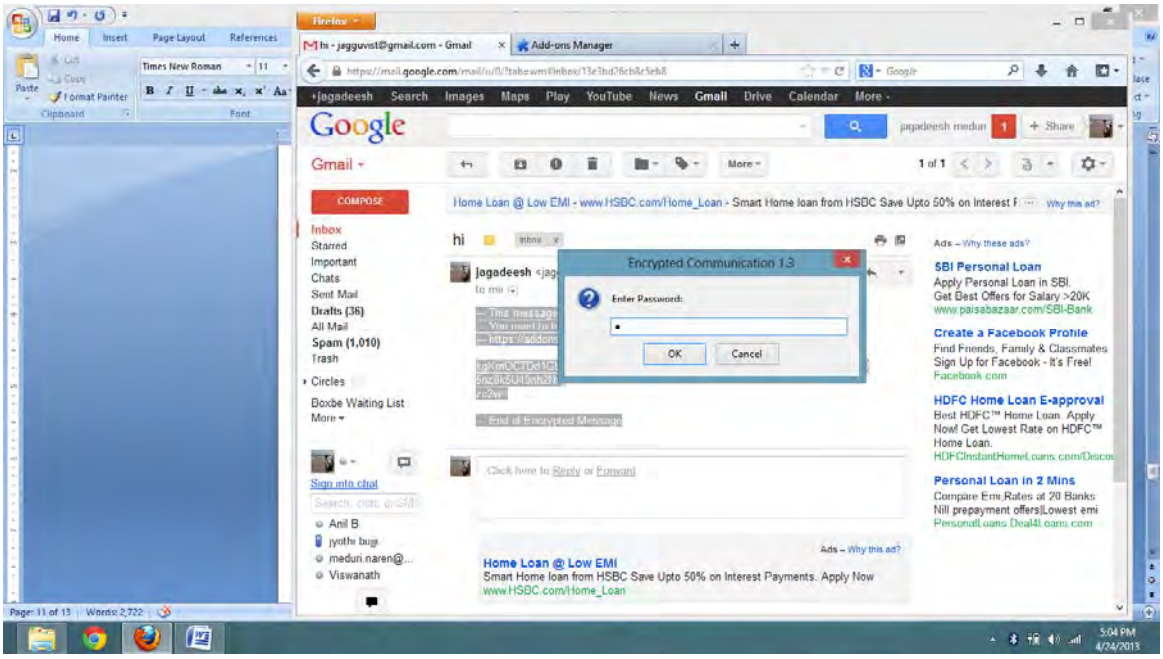

Figure 5 Decryption at receiver

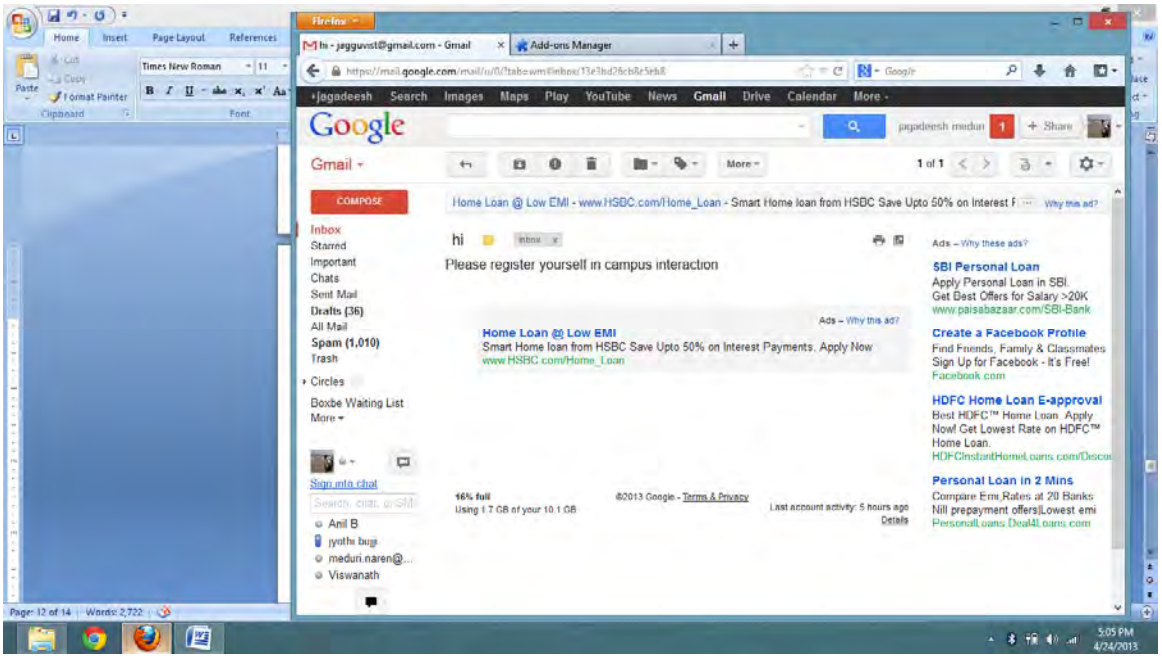

Figure 6 Original message

6. RESULTS

This model able to posses the following advantages in an effective manner

Table 1

Requirement	**Achieved by**
Confidentiality	Receiver is having secret key and add-on.
Integrity	By using hash as key instead of using key directly.
Authentication	Sharing secret key privately instead of mail.
Distributed Support	Add-on mechanism
System resources	Memory of the system in not used as in application oriented processes

7. FINDINGS

From the literature survey security models, it is understood, the designs that support application oriented mechanisms that too support particular operating system. But this proposed model overcomes the problem by add-on based which is independent of OS and accepted in Distributed Environment. It uses the AES encryption and decryption algorithm by Java script implementation. Browsers are following different file formats for add-ons. This create problem of installing the add-on in different browsers. Browsers should follow Universal add-on acceptability so that they can be used in any of the browsers. The complexity in add-on usage should be minimized and it should be made more users friendly for effective access.

This paper will give an idea to the research scholars and developers to design the universal acceptability designs which make the user to work with independent of the operating system they are using. The proposed model also compromises the reading of the user data by mail provided by encryption. The add-on creator can use different encryption algorithm and hash algorithm and make an Add-on and send data. It is hard for mail provider to find such activities.

8. CONCLUSION

From the proposed model a secure data communication model between two users using the Add-on is designed in a user friendly environment. The model was tested with the Mozilla Firefox and it satisfies all the security aspects user require like authentication, integrity and confidentiality, while performing data transfer between two machines. It will be useful in distributed environment and reduce OS involvement while performing data transactions in the cloud. Any OS can use these add-ons with a fixed web browser and also applicable to smart phones. Universal add-on's can be provided to browsing environment so that any add-on can be used in the any of the browser. This paper also gives clear idea how to design an add-on and motivates the developers to code through add-on for designing applications instead of building time and memory conserving software's.

References

[1] Cong Wang, Qian Wang, Wenjing Lou and Kui Ren, "Ensuring Data Storage Security in Cloud Computing", Quality of Service, 2009. IWQoS. 17th International Workshop.

[2] Farzad Sabahi, "Cloud computing security threats and responses", Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference.

[3] Md. Tanzim Khorshed, A.B.M. Shawkat Ali, Saleh A. Wasimi "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing", Future Generation Computer Systems, Volume 28, Issue 6, June 2012, Pages 833-851.

[4] Yong PENG, Wei ZHAO, Feng XIE, Zhong-hua DAI, Yang GAO, Dong-qing CHEN, "Secure cloud storage based on cryptographic techniques" , The Journal of China Universities of Posts and Telecommunications, Volume 19, Supplement 2, October 2012, Pages 182-189.

[5] Khaled Salah Jose M. Alcaraz Calero Jorge Bernal Bernabé Juan M. Marín Perez Sherali Zeadally, "Analyzing the security of Windows 7 and Linux for cloud computing", Computers & Security, Volume 34, May 2013, Pages 113-122.

[6] Saman Zonouz, Amir Houmansadr, Robin Berthier, Nikita Borisov, William Sanders "Secloud: A cloud-based comprehensive and lightweight security solution for smartphones", Computers & Security, 20 February 2013.

[7] Miao Zhou, Yi Mu, Willy Susilo, Jun Yan, Liju Don, "Privacy enhanced data outsourcing in the cloud", Journal of Network and Computer Applications, Volume 35, Issue 4, July 2012, Pages 1367-1373.

[8] Martin Gilje Jaatun, Gansen Zhao, and Stian Alapnes, "A Cryptographic Protocol for Communication in a Redundant Array of Independent Net-storages", Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference.

[9] Smith E and Ramgovind, "The Management of Security in Cloud Computing" published in Information Security for South Africa (ISSA), 2010.

[10] Sandeep K.Sood, "A combined approach to ensure data security in cloud computing", Journal of Network and Computer Applications, 2012.
[11] Eman M.Mohamed, Sherif EI-Etriby "Randomness Testing of Modem Encryption Techniques in Cloud Environment", Informatics and Systems (INFOS), 2012 8th International Conference.
[12] Qin Liu, Guojun Wang, Jie Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment" Information Sciences 26 October 2012.
[13] Tien-Cheu Kao, Ching-Hao Mao, Chien-Yu Chang and Kai-Chi Chang, "Cloud SSDLC: Cloud Security Governance Deployment Framework in Secure System Development Life Cycle", Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference.
[14] Said EL HAJJI and Abdellatif EL GHAZI "Homomorphic Encryption method applied to Cloud Computing", Network Security and Systems (JNS2), 2012.
[15] P.Varalakshmi, Hamsavardhini Deventhiran, "Integrity Checking for Cloud Environment Using Encryption Algorithm", Recent Trends In Information Technology (ICRTIT), 2012 International Conference.
[16] NIST, "Announcing the Advanced Encryption Standard (AES)" Federal Information, Processing Standards Publication 197, November 26, 2001.